CAIS-Alerta: Vulnerabilidade no kernel do Linux

[RNP, 18.08.2016]

O CAIS alerta para uma vulnerabilidade presente na implementação TCP do kernel do Linux. A falha está na implementação da RFC 5961, que é um padrão que determina como conexões TCP são estabelecidas entre hosts.

A exploração dessa vulnerabilidade permite a atacantes bloquearem a conexão entre dois hosts. Caso a conexão não seja cifrada, também há a possibilidade de injetar códigos maliciosos na comunicação. Esta capacidade de intervenção é capaz de burlar, inclusive, mecanismos de privacidade de redes como o Tor.

Até o momento da publicação deste alerta, não foram divulgados códigos de exploração para a vulnerabilidade listada.

Descrição

Um usuário mal intencionado pode controlar a conexão entre dois hosts de forma remota e inserir códigos maliciosos nesta comunicação.

O agravante é que não há a necessidade de se utilizar o ataque de "man-in-the-middle", ou seja, não é necessário interceptar a comunicação entre os dois hosts e forçar o tráfego de dados através de outro computador. Basta que a comunicação dure o tempo suficiente para ser interceptada (ao menos 60 segundos). O atacante também não precisa estar na mesma rede, pode se aproveitar da falha em qualquer lugar da internet.

Sistemas impactados

As versões do kernel do Linux a partir da v3.6 (inclusive) e anterior a v4.7

Correções disponíveis

Atualizar a versão do kernel do Linux para a versão 4.7.

*Caso não seja possível atualizar o sistema para essa versão do kernel, recomenda-se que a mitigação abaixo seja realizada:

1 - Editar o arquivo como root

/etc/sysctl.conf

2 - Incluir o conteúdo abaixo (em qualquer lugar) no arquivo

net.ipv4.tcp_challenge_ack_limit = 999999999

3 - Ativar a nova regra

sysctl –p

Identificadores CVE (https://cve.mitre.org)

CVE-2016-5696

Mais informações

https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_cao.pdf
http://thehackernews.com/2016/08/linux-tcp-packet-hacking.html
https://nakedsecurity.sophos.com/2016/08/12/researchers-announce-linux-kernel-network-snooping-bug/

O CAIS recomenda que os administradores mantenham seus sistemas e aplicativos sempre atualizados, de acordo com as últimas versões e correções oferecidas pelos fabricantes.
Os alertas do CAIS também são oferecidos no **Twitter**:

Siga @caisrnp